UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,535	02/16/2001	Norman H. Margolus	11656-002001	5190

26161 7590 06/16/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
PHAM, HUNG Q	

ART UNIT	PAPER NUMBER
2162	

DATE MAILED: 06/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/785,535	MARGOLUS ET AL.	
	Examiner	Art Unit	
	HUNG Q. PHAM	2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-10,12-60,62-67,98-159 and 175-186* is/are pending in the application.

4a) Of the above claim(s) *98-153* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-10,12-60,62-67,154-159 and 175-186* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

- The objection of claims 9 and 10 has been withdrawn due to the amendment of claim 9 and cancellation of claim 11.

- Applicants' request of withdrawing the rejection of claim 1 under 35 U.S.C § 112, first paragraph has been respectfully declined. Generally, applicants referred examiner to paragraphs [0046], [0047], and [0058] as the written description of the claimed ***relying on the data item already stored in the data repository for storage of the second data item rather than storing a separate copy of the second data item***. However, there is no description of the claimed ***relying on the data item already stored in the data repository for storage of the second data item rather than storing a separate copy of the second data item*** in these three paragraphs. Specifically, paragraphs [0046], [0047], and [0058] illustrate the concept of a single copy of data item in a repository, e.g., *like the BBS systems cited above, from a logical standpoint it contains only a single copy of each data-item stored in it no matter how many repository clients (i.e., computers running software acting on behalf of human users) store files into it containing the same data-item; to transfer such files to the repository, client software will typically only have to send a pointer, since the repository will already contain a copy of the data, sent earlier by some other client; logically only one copy of each distinct data-item is kept in the repository, which allows for great economy in use of storage space.*

- Applicants' arguments with respect to the rejection of claim 1 under U.S.C § 103 have been considered but are moot in view of the new ground(s) of rejection.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: ***physical storage nodes***, ***NFS file server***, ***CIFS file server***.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1 and 185 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As in claim 1, the step of ***relying on the data item already stored in the data repository for storage of the second data item rather than storing a separate copy of the second data item*** was not described in the specification.

As in claim 185, the technique of ***breaking up the record at boundaries that depend upon the content of the record*** was not described in the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1, 9, 175-178 and 180-186 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1] in view of Waters [USP 6,535,867 B1].

Regarding claim 1, Shnelvar teaches a method for storing data (Abstract).

As shown in FIG. 3, data from a data source 16 is processed for storing in Data Compression Storage Unit 52B of Data Repository 18 (Col. 15, Lines 33-42) as the step of ***having a first client program deposit a data item in a data repository.***

As shown in FIG. 4, step 54B, a Hash Value Generator 52AB as ***a reproducible pseudorandom process that produces digital fingerprints*** computes a Hash Value 58 or ***digital fingerprint*** for the data of each Data Unit 56 or ***data item*** generated from the data read from the Data Source 16 (Col. 17, Lines 56-58). In other words, step 54B performs the claimed ***determining a digital fingerprint from the data item using a reproducible pseudorandom process that produces digital fingerprints.***

If Hash Value 58 does not match a Hash Value 58 residing in an MDC Table 60. Container Manager 18d writes the data of the Data Unit 56 into a newly allocated Repository Allocation Unit 42R of the Data Compression Storage Unit 52B, wherein a Pointer 66 to the corresponding Repository Allocation Unit 42R associated with the Hash Value 58 is created (Col. 18, Lines 23-40). As seen, ***the data item is stored in the data repository*** 18 ***at a*** newly allocated Repository Allocation Unit 42R as ***physical location or location associated with the*** Hash Value 58 as ***digital fingerprint.***

As shown in FIG. 1, system 10 comprises multiple User Systems 12, whereupon the Data Repository 18 will reside in a selected User Systems 12 while the Data Source 16 may be comprised of one or more User Systems 12 (Col. 16, Lines 12-20). Thus, at another particular time, after a particular User System 12 storing data in Data Repository 18 as discussed above, another User System 12 as ***a second client program initiates a process for depositing*** it own Data Source 16 comprises ***second data item in the Data***

Repository 18, *wherein* a duplicate of the data in the Data Unit 56 may already reside in the Data Repository 18, or ***the second data item is identical to the data item stored by the first client program.***

Shnelvar further discloses the step of ***determining a digital fingerprint from the second data item using the reproducible pseudorandom process*** (FIG. 4, step 54B, Col. 17, Lines 56-58);

comparing the digital fingerprint from the second data item to digital fingerprints for data items already stored in the data repository (FIG. 4, step 54C, Col. 18, Lines 4-11), and ***determining from the comparing of digital fingerprints that a data item identical to the second data item is already stored in the data repository*** (Col. 18, Lines 41-44)

When the Hash Value 58 of a Data Unit 56 matches a Hash Value residing in an MDC Table 60 (Col. 18, Lines 41-44), Data Unit 56 and its Hash Value 58 are stored into a Suspense Element 68a of a Suspense Array 68b for subsequent processing. Suspense Processor 52AE compares the data of the suspended Data Unit 56 with the data read from the Resource Allocation Unit 42R. If the data of the suspended Data Unit 56 is found not to match the data of the Resource Allocation Unit 42R, the data of the suspended Data Unit 56 is written into a newly allocated Repository Allocation Unit 42R of DCSU 52B. If the data of the of the suspended Data Unit 56 is found to match the data read from the Resource Allocation Unit 42R, the suspended Data Unit 56 is discarded as being a duplicate of data already existing in a Repository Allocation Unit 42R (Col. 18, Line 56-Col. 19, Line 18). As seen, the technique of comparing the data of Data Unit 56 with data already stored in the data repository for storage rather storing a

separate copy indicates the step of ***relying on the data item already stored in the data repository for storage of the second data item rather than storing a separate copy of the second data item.***

Shnelvar further discloses the Hash Value is a 32-bit hash value generated by a CRC32 algorithm. If the number of bits in a hash is 32 bits and the hash values are uniformly distributed across the possible input values then one would expect a hash value collision once every 2^{16} or 65,536 hash key value generations. The hashing algorithm and size of hash values are selected, for any given implementation, so that the number of bits used in the hash values relative to the number of allocation units is such that the likelihood that non-identical data units will result in identical hash values is significantly reduced, so that such occurrences will be relatively rare (Col. 21, Lines 49-67). As seen, the CRC32 algorithm as ***a reproducible pseudorandom process*** is adapted to guarantee one collision out of 65,536 hash key value generations as ***probabilistically guarantee*** to provide a ***unique*** hash value as ***digital fingerprint*** to every data unit sending to the data repository. In short, ***the reproducible pseudorandom process produces a digital fingerprint adapted to probabilistically guarantee to provide a unique digital fingerprint for every distinct data item sent to the data repository***, and because the hash values created by CRC32 has a statistical randomness, the hash values as ***digital fingerprints have a pseudorandom distribution.***

When the Hash Value 58 of a Data Unit 56 matches a Hash Value 58 residing in an MDC Table 60. It is possible for the Repository Allocation Unit 42R to have the same Hash Value 58 and yet have different contents (Col. 18, Lines 41-46). To add a new entry to the MDC Record 62 and store the Data Unit 56 in a Resource Allocation Unit

42R of Data Repository 18 if a match was not found. The Data Repository 18 is structured into Containers 18a and Compartments 18b, and Data Units 56 are stored in the Repository Allocation Units 42R of one or more Compartments 18b of Containers 18a of Data Repository 18, so that entries in MDC Record 62 will point into the Container 18a structures (Col. 25, Lines 2-13). As seen, the hash value of a data unit is also the hash value of Resource Allocation Unit that stores the data unit, and obviously, the ***pseudorandom distribution*** of the hash value or ***digital fingerprint***, as discussed above, also places upon the hash value of the Repository Allocation Units or ***the physical storage nodes at which data items are stored in the data repository*** as well.

The difference between the claimed invention and Shnelvar method is technique of ***without comparing the entire contents of the second data item to the entire contents of a data item already stored.***

Waters teaches a method for computing a hash value of a file name; Waters further discloses the technique of ignoring the hashing collisions to avoid the step of ***comparing the entire contents of the second data item to the entire contents of a data item already stored*** (Waters, Col. 7, Lines 45-53).

It would have been obvious for one of ordinary skill in the art at the time the invention was made to ignore the hashing collisions as taught by Waters to avoid the step of string comparing in order to reduce the time that needed to perform the process.

Regarding claim 9, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 2, Shnelvar further discloses

one or more additional copies or other forms of redundant information about the data items is stored in the data repository for data integrity, availability, or accessibility purposes and not to provide separate storage of the data item for different client programs (Shnelvar, Col. 11, Line 64-Col. 12, Line 22).

Regarding claim 175, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further discloses ***physical storage nodes each comprise one or more different hard disk drives*** (Shnelvar, FIG. 1).

Regarding claim 176, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further discloses ***the physical storage nodes each comprise one or more different data servers*** (Shnelvar, FIG. 3, Col. 16, Lines 21-34).

Regarding claim 177, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further discloses ***the physical storage nodes each comprise one or more different processors*** (Shnelvar, Col. 16, Lines 21-34).

Regarding claim 178, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further

discloses ***the data repository comprises physical storage nodes linked by a network*** (Shnelvar, FIG. 3).

Regarding claim 180, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further discloses ***the first and second client programs are independent programs*** (Shnelvar, Col. 16, Lines 12-20).

Regarding claim 181, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 180, Shnelvar further discloses ***the independent programs are running on separate computers*** (Shnelvar, Col. 16, Lines 12-20).

Regarding claim 182, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further discloses ***the first and second client programs are the same program running at different times*** (Shnelvar, Col. 16, Lines 8-12).

Regarding claim 183, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, Shnelvar further discloses ***the first client program comprises an NFS or CIFS file server*** (Shnelvar, FIG. 3).

Regarding claim 184, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, but do not explicitly teach ***files and directories are named objects within the data repository***. However, the technique of representing files and directories by names is a conventional method and implied in Shnelvar and Water technique in order to hash a file name including the path or directory using a hash function.

Regarding claim 185, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, but do not teach ***data item comprises a component of a record, and the component is formed by breaking up the record at boundaries that depend upon the content of the record***. However, table is a conventional data structure for storing data, e.g., table as in FIG. 7, wherein a column is a component of a record, and a column of a table is formed by breaking up the record at boundaries that depend upon the content of the record.

Regarding claim 186, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 185, FIG. 7 of Shnelvar further implies ***the record is a file or a portion of a database***.

Claims 10, 12-17, 19, 54-56 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1] and Waters [USP 6,535,867 B1] as applied to claim 1 above, and further in view of Thorsen [USP 6,052,688].

Regarding claim 10, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, and further discloses the step of ***associating the data item with each of a plurality of access-authorization credentials***, but fails to teach ***each of which is uniquely associated with a particular user or client program***. Thorsen teaches the technique of ***associating the data item with a particular user or client program*** (Thorsen, Col. 10, Line 42-Col. 11, Line 5). It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar technique by including the step of associating access credential with a particular user in order to control access to a file or document.

Regarding claim 12, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 10, Thorsen further discloses the step of ***storing a plurality of named objects, each named object comprising information representative of the data item paired with information representative of one of the access-authorization credentials*** (Thorsen, Col. 10, Line 42-Col. 11, Line 5).

Regarding claim 13, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 12, Shnelvar further discloses ***the information representative of the data item is a digital fingerprint*** (Shnelvar, Col. 18, Lines 4-22).

Regarding claim 14, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 12, Shnelvar further discloses ***the information representative of the access authorization credential is a cryptographic hash of all or part of the access-authorization credential*** (Shnelvar, Col. 18, Lines 4-22).

Regarding claim 15, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 14, Shnelvar further discloses ***the cryptographic hash is an access identifier that uniquely identifies the data item for a particular user or client program*** (Shnelvar, Col. 18, Lines 4-22).

Regarding claim 16, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 12, Shnelvar further discloses ***the named object is a data structure created by the client program*** (Shnelvar, Col. 18, Lines 4-22).

Regarding claim 17, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 12, Shnelvar further discloses ***the named object is a data structure created by a server program acting on behalf of the repository*** (Shnelvar, Col. 18, Lines 4-22).

Regarding claim 19, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 12, Shnelvar further discloses ***a client retrieving a data item by accessing a named object using an access-authorization credential to select the named object, and using the contents of the named object to determine the location of the data item in the data repository*** (Shnelvar, Col. 18, Line 56-Col. 19, Line 18).

Regarding claim 54, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 12, Shnelvar further discloses a data item is represented as a ***composite of data-items, and the component data-items are separately deposited in the repository*** (Shnelvar, Col. 17, Lines 42-55).

Regarding claim 55, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 54, Shnelvar further discloses ***lists of fingerprints for data-items making up a composite data-item are deposited as an index data item, which can be given an object-name and used for obtaining access to any of the component data-items*** (Shnelvar, Col. 18, Lines 4-22).

Regarding claim 56, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 55, but does not disclose ***a proof-of-deposit is returned for each component deposit, and some or all of the proofs are presented when the index data item is given an object-name.*** However, a message return to a

user when the process is finished in step 54F of FIG. 4 is well known in the art, and similar to the message disclosed by Thorsen in Col. 11, Lines 53-55. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to include a proof of deposit in order to notify a user a process is completed.

Regarding claim 60, Shnelvar, Waters and Thorsen, in combination, teach all of the claimed subject matter as discussed above with respect to claim 15, Shnelvar further discloses ***the physical location at which information about named-objects is stored is based on access identifiers*** (Shnelvar, Col. 18, Lines 41-46 and Col. 25, Lines 2-13), but not explicitly discloses the claimed ***to introduce reproducible pseudorandomness into the physical locations of the items***. However, as taught by Shnelvar, when the Hash Value 58 of a Data Unit 56 matches a Hash Value 58 residing in an MDC Table 60. It is possible for the Repository Allocation Unit 42R to have the same Hash Value 58 and yet have different contents (Col. 18, Lines 41-46). To add a new entry to the MDC Record 62 and store the Data Unit 56 in a Resource Allocation Unit 42R of Data Repository 18 if a match was not found. The Data Repository 18 is structured into Containers 18a and Compartments 18b, and Data Units 56 are stored in the Repository Allocation Units 42R of one or more Compartments 18b of Containers 18a of Data Repository 18, so that entries in MDC Record 62 will point into the Container 18a structures (Col. 25, Lines 2-13). As seen, the hash value of a data unit is also the hash value of Resource Allocation Unit that stores the data unit, and obviously, the ***pseudorandom distribution*** of the hash value or ***digital fingerprint***, as discussed above, also places upon the hash value of the

Repository Allocation Units or ***the physical location at which data items are stored in the data repository*** as well. It would have been obvious for one of ordinary skill in the art at the time the invention was made to introduce pseudorandomness into the physical location in order to reduce identical hash values.

Claims 18, 20, 21, 29, 30, 32, 52, 53, 57 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1] and Thorsen [USP 6,052,688] as applied to claims 10 and 12 above, and further in view of Whiting et al. [USP 5,778,395].

Regarding claim 18, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 12, but fails to disclose ***a client replacing an existing version of a named object with a new version of that named object, by replacing the existing association with a data item stored in the data repository with a new association***. Whiting teaches a method for backing up files, Whiting further discloses the differences between a file and its version in the previous backup may be computed so that only the changes to the file need to be written on the backup storage means (Whiting, Col. 5, lines 3-26). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thorsen method by including the step of replacing an existing version by replacing the association with a data item in order to back up file to a backup storage means.

Regarding claim 20, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 12, but fails to teach ***the named objects further comprise version information associating different data items with different versions of the named object***. Whiting teaches a method for backing up files, Whiting further discloses ***the named objects further comprise version information associating different data items with different versions of the named object*** (Whiting, Col. 9, line 56-Col. 10, line 65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thorsen method by including the technique of version information in order to differentiate data.

Regarding claim 21, Shnelvar, Waters, Thorsen and Whiting teaches all the claimed subject matters as discussed in claim 20, Whiting further discloses ***a backup of data items stored in the data repository is accomplished by preserving copies of the current versions of named objects in existence at the time of the backup*** (Whiting, Col. 7, line 59-Col. 8, line 20).

Regarding claim 29, Shnelvar, Waters, Thorsen and Whiting teaches all the claimed subject matters as discussed in claim 20, Whiting further discloses the step of ***preparing a digital time stamp of a plurality of named objects to allow a property of these named objects to be proven at a later date*** (Whiting, Col. 12, lines 38-48).

Regarding claim 30, Shnelvar, Waters, Thorsen and Whiting teaches all the claimed subject matters as discussed in claim 29, Whiting further discloses ***a random or other difficult to guess element is incorporated into the time stamp hash for each named object, to***

prevent the property form being proven if this element is deleted (Whiting, Col. 28, line 35-Col. 29, line 9).

Regarding claim 32, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 12, but fails to disclose the step of ***altering one or more properties or parameters associated with an access-authorization credential to change the access rights of a client or user to the data item referenced by that credential***. Whiting teaches a method for backing up files, Whiting further discloses the step of ***altering one or more properties or parameters associated with an access-authorization credential to change the access rights of a client or user to the data item referenced by that credential*** (Whiting, Col. 7, lines 32-58). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thorsen method by including the step of altering one or more properties to change the access right in order to control access to the data.

Regarding claim 52, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 10, but fails to disclose ***the access –authorization credential is determined in part by computing a hash involving elements of the pathname for a file on the client computer***. Whiting teaches a method for backing up files, Whiting further discloses ***the access –authorization credential is determined in part by computing a hash involving elements of the pathname for a file on the client computer*** (Whiting, Col. 15, line 58-Col. 16, line 17). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong and Brady method by using the technique of computing a hash involving the pathname in order to back up image dataset.

Regarding claim 53, Shnelvar, Waters, Thorsen and Whiting teaches all the claimed subject matters as discussed in claim 52, Whiting further discloses ***the path name hash is made unique to a client by introducing a reproducible but randomly chosen element into it*** (Whiting, Col. 15, lines 58-Col. 16, line 17).

Regarding claim 57, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 56, but fails to disclose ***when transmitting a composite data-item, the client uses fingerprints to avoid retransmitting components following loss of communication***. Whiting teaches a method for backing up files, Whiting further discloses ***when transmitting a composite data-item, the client uses fingerprints to avoid retransmitting components following loss of communication*** (Whiting, Col. 5, lines 3-34). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thorsen method by using fingerprint to avoid retransmitting in order to reduce the network bandwidth.

Regarding claim 58, Shnelvar, Waters, Thorsen and Whiting teaches all the claimed subject matters as discussed in claim 57, Shnelvar further discloses ***the index data-item is encrypted with a key that is only made available to the repository at the moment of access*** (Shnelvar, FIG. 4).

Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Thorsen [USP 6,052,688] as applied to claim 12, and further in view of Garthwaite et al. [USP 6,415,302 B1].

Regarding claim 31, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 12, but fails to disclose the step of ***determining that a data item stored in the data repository is not referenced by any named object, and reusing the storage space used to store the unreferenced data item***. Garthmaite teaches a garbage collection method by ***determining that a data item stored in the data repository is not referenced by any named object, and reusing the storage space used to store the unreferenced data item*** (Garthmaite, Col. 5, line 14-Col. 6, line 8). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thorsen method by using the garbage collection method as taught by Garthmaite in order to free unused memory.

Claims 7, 22-28, 33-39, 47, 48, 50, 51, 154-156, 158 and 159 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1] as applied to claim 1 above, and further in view of Whiting et al. [USP 5,778,395].

Regarding claim 22, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but fails to teach ***records are kept of the association between***

data items and names in order to define named objects, and wherein data items recorded as being associated with named objects are not deleted from the repository, and wherein named objects are backed up by preserving copies of the named object records in existence at the time of the backup. Whiting teaches a method for backing up files, Whiting further discloses ***records are kept of the association between data items and names in order to define named objects, and wherein data items recorded as being associated with named objects are not deleted from the repository, and wherein named objects are backed up by preserving copies of the named object records in existence at the time of the backup*** (Whiting, Col. 7, line 59-Col. 8, line 20). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar method by using the technique of defining named objects and preserving copies of the named objects in order to back up data.

Regarding claim 23, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 22, Whiting further discloses ***a plurality of backups are made at spaced time intervals*** (Whiting, Col. 1, lines 30-50).

Regarding claim 24, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 22, Whiting further discloses ***the backup is accomplished by declaring that after a prescribed moment in time a new version of each named object will be created the first time that a new data item is associated with it*** (Whiting, Col. 7, line 59-Col. 8, line 20).

Regarding claim 25, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 24, Whiting further discloses ***the prescribed moment in time is determined separately for each named object*** (Whiting, Col. 7, line 59-Col. 8, line 20).

Regarding claim 26, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 22, Whiting further discloses ***named objects are preserved by creating a new version of each named object each time that a new data item is associated with it*** (Whiting, Col. 8, lines 21-40).

Regarding claim 27, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 26, Whiting further discloses ***versions of named objects that are deemed unnecessary are deleted*** (Whiting, Col. 25, lines 9-39).

Regarding claim 28, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 27, Whiting further discloses ***the determination of which versions of a named object to delete is based in whole or in part on the times at which the versions were created, and the intervals between these times*** (Whiting, Col. 25, lines 9-39).

Regarding claim 33, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but fails to disclose ***a challenge step to ascertain that the client has the full data item***. Whiting teaches a method for backing up files, Whiting further discloses ***a challenge step to ascertain that the client has the full data item*** (Whiting, Col. 35,

lines 8-63). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar method by including a challenge step as taught by Whiting in order to control access to data.

Regarding claim 34, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 33, Whiting further discloses the step of ***requiring that the client attempting to store a data item provide correct answers to inquiries as to the content of portions of the data item, or inquiries that require knowledge of this content*** (Whiting, Col. 35, line 64-Col. 36, line 4).

Regarding claim 35, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 34, Whiting further discloses ***the data item content on which the challenge is based is selected with a degree of randomness*** (Whiting, Col. 35, line 64-Col. 36, line 4).

Regarding claim 36, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but fails to disclose ***depositors use the client to stored data items in the repository, and at least some depositors are required to provide identification***. Whiting teaches a method for backing up files, Whiting further discloses ***depositors use the client to stored data items in the repository, and at least some depositors are required to provide identification*** (Whiting, Col. 35, lines 7-43). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar method by

including the requiring identification of depositors to store data items in order to control access to data.

Regarding claim 37, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 36, Whiting further discloses ***rules for when a depositor must provide identification are selected in order to discourage unlawful distribution of access to the data item*** (Whiting, Col. 35, lines 7-43).

Regarding claim 38, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 37, Whiting further discloses ***there is a greater degree of user identification or a higher likelihood that user identification will be required when the data item being stored by the depositor has been indicated to be shareable with other users*** (Whiting, Col. 28, line 35-Col. 29, line 10).

Regarding claim 39, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 37, Whiting further discloses ***a class of data items the items may only be shared if the depositor has provided adequate identification*** (Whiting, Col. 28, line 35-Col. 29, line 10).

Regarding claim 47, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but fails to disclose ***the client has a directory structure for the data items, the data items are stored in the repository, and the directory structure is not evident to the repository maintainers***. Whiting teaches a method for backing up files, Whiting further

discloses ***the client has a directory structure for the data items, the data items are stored in the repository, and the directory structure is not evident to the repository maintainers*** (Whiting, Col. 4, lines 19-45). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar method by including a directory structure for data items in order to back up data.

Regarding claim 48, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but fails to disclose ***the client program using the repository is a mirroring program which determines which data items to deposit in the repository, and wherein that determination is based at least in part on the result of a comparison of digital fingerprints establishing that certain data items are not in the repository***. Whiting teaches a method for backing up files, Whiting further discloses ***the client program using the repository is a mirroring program which determines which data items to deposit in the repository, and wherein that determination is based at least in part on the result of a comparison of digital fingerprints establishing that certain data items are not in the repository*** (Whiting, Col. 7, line 59-Col. 9, line 10). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar method by including the step of determining which data items to deposit in the repository based on at least in part on the result of a comparison in order to back up data.

Regarding claim 50, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 48, Whiting further discloses ***the default for deciding***

what data items to mirror is to mirror all or substantially all data items (Whiting, Col. 7, line 59-Col. 8, line 40).

Regarding claim 51, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 48, Whiting further discloses the step of ***making a determination of which data items need to be transmitted to the repository, and wherein that determination is based primarily on a comparison of digital fingerprints for data items at the client and data items in the repository*** (Whiting, Col. 18, line 66-Col. 19, line 53).

Regarding claim 154, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but does not disclose the step of ***encrypting the data item using a key derived form the content of the data item***. Whiting teaches a method for backing up files, Whiting further discloses the step of ***encrypting the data item using a key derived form the content of the data item*** (Whiting, Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to include the step of encrypting as taught by Whiting in order to secure the transferring data.

Regarding claim 155, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but does not disclose the step of ***encrypting the data item using a key derived form the content of the data item***. Whiting teaches a method for backing up files, Whiting further discloses the step of ***encrypting the data item using a key derived form the***

content of the data item (Whiting, Col. 26, Line 66-Col. 27, Line 6, and Col. 28, Lines 35-65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to include the step of encrypting as taught by Whiting in order to secure the transferring data.

Regarding claim 156, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, but does not explicitly disclose ***the data items are widely circulated non-electronic media such as books or music, and the method further comprises converting the widely circulated non-electronic media to a standardized electronic version; storing the standardized electronic version as a data item in the repository; promoting the availability of the standardized electronic version to users with the right to have access, whereby the likelihood of the data repository storing multiple, slightly-different electronic versions of the non-electronic media is reduced.*** However, the technique of promoting the electronic data item to user with the right to have access is taught by Whiting (Col. 26, Line 66-Col. 27, Line 6, and Col. 28, Lines 35-65). A non-electronic media such as books could be converted to a standardized electronic version by using a conventional method such as directly typing or scanning and saving the data in a repository under word perfect for example in order to standardized the file, obviously, will reduce the likelihood of different version. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar technique by converting a non-electric media to a standardized electronic version and having access right in order to reduce the storage space of book in paper version and secure the data item.

Regarding claim 158, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 48, Shnelvar further discloses ***a mirroring capability for a personal computer, and mirroring software for carrying out the method is initially configured to mirror essentially all data on the user's computer*** (Shnelvar, FIG. 1, Col. 1-2).

Regarding claim 159, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 48, but does not explicitly teach ***a mirroring capability for a wireless network device.*** However, a wireless network device such as a computer is well known in the art. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Whiting technique by including a wireless network device in order to back up data from a wireless node.

Regarding claim 7, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 154, Whiting further discloses ***the key derived from the content of the data item is the same for all instances of the data item stored in the repository*** (Whiting, Col. 26, Line 66-Col. 27, Line 6, and Col. 28, Lines 35-65).

Claims 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Whiting et al. [USP 5,778,395] as applied to claim 38, and further in view of Ho [USP 6,148,342].

Regarding claim 40, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 38, but fails to disclose ***identity information about the depositor is made available to anyone able to access the data item, to discourage unlawful sharing***. Ho teaches a method for managing sensitive data and further discloses ***identity information about the depositor is made available to anyone able to access the data item***. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong, Brady and Whiting method by including the step of disclosing the identity information to discourage unlawful sharing in order to prevent unauthorized access to data.

Regarding claim 41, Shnelvar, Waters, Whiting, and Ho teaches all the claimed subject matters as discussed in claim 40, Whiting further discloses ***the identity information is stored in an encrypted form that the depositor and users subsequently accessing the shared data item can both read*** (Whiting, Col. 28, lines 36-65).

Regarding claim 42, Shnelvar, Waters, Whiting, and Ho teaches all the claimed subject matters as discussed in claim 41, Whiting further discloses ***the repository is not able to decrypt the identity information about the depositor*** (Whiting, Col. 29, lines 10-21).

Claims 43-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Whiting et al. [USP 5,778,395] as applied to claim 37, and further in view of Deo [USP 5,594,227].

Regarding claim 43, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 37, but fails to disclose ***the identity of some users has not been well verified, but restrictions are placed on sharing of data item deposited by such poorly verified users***. Deo teaches a method for protecting against unauthorized access of data contents by denying access to data contents on a smart card (Deo, FIG. 7) as the ***identity of some users has not been well verified, but restrictions are placed on sharing of data item deposited by such poorly verified users***. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Whiting method by using the technique of placing restriction on data deposited by poorly verified users in order to control access to data.

Regarding claim 44, Shnelvar, Waters, Whiting and Deo teaches all the claimed subject matters as discussed in claim 43, Deo further discloses the step of ***limiting access to data items deposited by a poorly verified user*** (Deo, FIG. 7).

Regarding claim 45, Shnelvar, Waters, Whiting and Deo teaches all the claimed subject matters as discussed in claim 44, Deo further discloses ***the limited access is provided by limiting the aggregate bandwidth provided for such accesses*** (Deo, FIG. 7).

Regarding claim 46, Shnelvar, Whiting and Deo teaches all the claimed subject matters as discussed in claim 44, Deo further discloses ***the limited access is provided by limiting the number of simultaneous accesses to the data items*** (Deo, FIG. 7).

Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Whiting et al. [USP 5,778,395] as applied to claim 48, and further in view of Dobbek [USP 6,308,325 B1].

Regarding claim 49, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 48, but fails to disclose ***mirroring software is downloaded to the client using a bootstrap process, wherein a small bootstrap program is downloaded and executed, and the bootstrap program manages download and installation of the remainder of the mirroring software***. Dobbek teaches a method for downloading data, Dobbek further discloses ***software is downloaded to the client using a bootstrap process, wherein a small bootstrap program is downloaded and executed, and the bootstrap program manages download and installation of the remainder of the mirroring software*** (Dobbek, Col. 5, line 60-Col. 6, line 40, and Col. 2, lines 23-43). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Whiting method by downloading a bootstrap process for managing downloading and installing the software in order to have a software to control back up data.

Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Thorsen [USP 6,052,688] as applied to claim 55 above, and further in view of Kuzma [USP 5,781,901].

Regarding claim 59, Shnelvar, Waters and Thorsen teaches all the claimed subject matters as discussed in claim 55, but fails to disclose ***an email message is broken up into component items in such a manner that the individual attachments are separate component data-items***. Kuzma teaches a method for transmitting email attachments form a sender to a receiver of a network. Kuzma further discloses ***the email message is broken up into component items in such a manner that the individual attachments are separate component data-items*** (Kuzma, Col. 4, line 65-Col. 5, line 65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thorsen method by using the technique of breaking an email into component items based on attachment in order to secure the message.

Claims 62, 63 and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1] as applied to claim 1, and further in view of Thomlinson et al. [USP 6,532,542 B1].

Regarding claim 62, Shnelvar and Waters teaches all the claimed subject matters as discussed in claim 1, Shnelvar fails to disclose ***an access identifier is formed to provide proof of ownership of the data item stored in the repository, the access identifier is formed by producing a one-way hash including item-identifying information chosen by the client program to***

identify the data item, and the one-way hash cannot be reversed to permit the repository to discover the identity of the client program or user. Thomlinson teaches a method to provide central storage for data items. Thomlinson further discloses ***an access identifier is formed to provide proof of ownership of the data item stored in the repository, the access identifier is formed by producing a one-way hash including item-identifying information chosen by the client program to identify the data item, and the one-way hash cannot be reversed to permit the repository to discover the identity of the client program or user*** (Thomlinson, Col. 10, line 43-Col. Col. 11, line 32 and Col. 7, lines 45-67). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar method by using a one-way hash to produce password as access identifier in order to control access to data.

Regarding claim 63, Shnelvar, Waters and Thomlinson teaches all the claimed subject matters as discussed in claim 62, Thomlinson further discloses ***the item-identifying information is associated with the data item on the client*** (Thomlinson, FIG. 3).

Regarding claim 65, Shnelvar, Waters and Thomlinson teaches all the claimed subject matters as discussed in claim 62, Thomlinson further discloses ***user-identifying information is provided to the repository as part of the access-authorization credential*** (Thomlinson, FIG. 3).

Claims 64, 66 and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1],

Thomlinson et al. [USP 6,532,542 B1] as applied to claim 63, and further in view of Whiting et al. [USP 5,778,395].

Regarding claim 64, Shnelvar and Thomlinson teaches all the claimed subject matters as discussed in claim 63, but fails to disclose ***the item-identifying information is derived at least in part from the path name of the data item on the client.*** Whiting teaches a method for backing up files, Whiting further discloses the ***item-identifying information is derived at least in part from the path name of the data item on the client*** (Whiting, Col. 15, line 58-Col. 16, line 17). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thomlinson method by using the technique of computing a hash involving the pathname in order to back up image dataset.

Regarding claim 66, Shnelvar, Waters and Thomlinson teaches all the claimed subject matters as discussed in claim 65, but fails to disclose ***at least some access-authorization credentials can be transferred between users without the use of the repository.*** Whiting teaches a method for backing up files, Whiting further discloses ***at least some access-authorization credentials can be transferred between users without the use of the repository*** (Whiting, Col. 28, lines 35-65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thomlinson method by using the technique of transferring access-authorization credentials as taught by Whiting in order to back up data in a share file server.

Regarding claim 67, Shnelvar, Waters and Thomlinson teaches all the claimed subject matters as discussed in claim 65, but fails to disclose ***at least one class of users is not permitted to transfer access using access-authorization credentials***. Whiting teaches a method for backing up files, Whiting further discloses ***at least one class of users is not permitted to transfer access using access-authorization credentials*** (Whiting, Col. 29, lines 1-9). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Thomlinson method restricting one class of users for transferring access as taught by Whiting in order to protect the privacy of the data.

Claim 4-6 and 157 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Whiting et al. [USP 5,778,395] as applied to claim 48, and further in view of the Admission [Background].

Regarding claim 157, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 48, Shnelvar further discloses ***a mirroring capability for a personal computer*** (Shnelvar, FIG. 1), but not to teach the claimed ***mirroring software with instructions for carrying out the aforesaid steps is preconfigured on the personal computer upon purchase***. In the background is an amount of fee for providing a combination of PC software and networked storage space that allows users to keep a copy of their most important data remotely from some company. Therefore, it would have been obvious for

one of ordinary skill in the art at the time the invention was made to impose a fee on the users who use the system in order to maintain the system.

Regarding claim 4, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 1, but does not disclose ***the encrypting of the data item is performed by the client prior to transmitting the data item to the data repository***. In the background is the technique of performing the encrypting of the data item prior to transmitting (Background). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to encrypt the data prior to transmitting in order to secure the data item.

Regarding claim 5, Shnelvar, Waters, Whiting and the admission teaches all the claimed subject matters as discussed in claim 4, Whiting further discloses the step of ***encrypting the key and storing the encrypted key*** (Whiting, Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding claim 6, Shnelvar, Waters, Whiting and the admission teaches all the claimed subject matters as discussed in claim 5, Whiting further discloses ***a client or user specific key is used to encrypt the key derived from the content of the data item*** (Whiting, Col. 26, Line 66-Col. 27, Line 6, and Col. 28, Lines 35-65).

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1], Whiting et al. [USP 5,778,395] as applied to claim 154, and further in view of Pond et al. [USP 4,864,616].

Regarding claim 8, Shnelvar, Waters and Whiting teaches all the claimed subject matters as discussed in claim 154, but fails to disclose ***users of the method are grouped into families, and the key derived from the content of the data item is the same for all instances of the data item stored in the repository by users in the same family, but may be different for users in different families***. Pond teaches a method of cryptographically labeling electronically stored data and further discloses ***users of the method are grouped into families, and the key derived from the content of the data item is the same for all instances of the data item stored in the repository by users in the same family, but may be different for users in different families*** (Summary, Col. 2-4). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Shnelvar and Whiting method by grouping the users into families and using the same key for users in the same family as taught by Pond in order to control access to data.

Claim 179 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shnelvar [USP 6,374,266 B1], Waters [USP 6,535,867 B1] as applied to claim 1 above, and further in view of the Admission [Background].

Regarding claim 179, Shnelvar and Waters, in combination, teach all of the claimed subject matter as discussed above with respect to claim 1, but fail to teach the technique of ***transmitting over the network the digital fingerprint of the second data item rather than the second data item itself.*** As disclosed in the Background is the technique of ***transmitting over the network the digital fingerprint of the second data item rather than the second data item itself*** (Background, page 2, line 24-page 3, line 5). It would have been obvious for one of ordinary skill in the art at the time the invention was made to transmit the digital fingerprint rather than the data item as taught in the Admission in order to reduce the transferring time.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HUNG Q. PHAM whose telephone number is 571-272-4040. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOHN E. BREENE can be reached on 571-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HUNG Q PHAM
Examiner
Art Unit 2162

May 31, 2005

SHAHID ALAM
PRIMARY EXAMINER